In the Claims

This listing of claims will replace all prior versions, and listings, of claims in the application:

What is Claimed:

1. (Currently Amended) A smartcard transaction system configured with a biometric security ~~system~~ device, said system comprising:

a smartcard configured to communicate with a reader wherein said reader and said biometric security device are configured to communicate with a host;

~~a reader configured to communicate with said system; and~~

said biometric security device comprises a fingerprint sensor to detect a proffered fingerprint sample, said fingerprint sensor configured to communicate with said ~~system~~ host; ~~and~~

a verification device configured to ~~verify~~ compare said proffered fingerprint sample with a registered fingerprint sample, wherein said registered fingerprint sample is primarily associated with a first user account and secondarily associated with a second user account, and wherein said second user account is different than said first user account ~~to facilitate a transaction~~; and

wherein said smartcard is configured to utilize at least one of said first user account and said second user account to facilitate a smartcard payment transaction.

2. (Currently Amended) The smartcard transaction system of claim 1, wherein said ~~sensor~~ biometric security device is configured to communicate with said ~~system~~ host via at least one of ~~a~~ said smartcard, ~~a~~ said reader, and a network.

3. (Original) The smartcard transaction system of claim 1, wherein said fingerprint sensor is configured to facilitate a finite number of scans.

4. (Currently Amended) The smartcard transaction system of claim 1, wherein said fingerprint sensor is configured to store log data comprising at least one of a detected fingerprint sample, processed fingerprint sample and ~~stored~~ registered fingerprint sample, and wherein said fingerprint sensor is further configured to employ a security procedure when said proffered fingerprint sample differs from said log data.

5. (Original) The smartcard transaction system of claim 1, further including a database configured to store at least one data packet, wherein said data packet includes at least one of proffered and registered fingerprint samples, proffered and registered user information, terrorist information, and criminal information.

6. (Currently Amended) The smartcard transaction system of claim 5, wherein said database is contained in at least one of ~~the~~ said smartcard, ~~smartcard~~ said reader, said fingerprint sensor, a remote server, a merchant server and said smartcard transaction system.

7. (Currently Amended) The smartcard transaction system of claim 6, wherein said ~~remote~~ database is configured to be operated by an authorized sample receiver.

8. (Currently Amended) The smartcard transaction system of claim 1, wherein said fingerprint sensor ~~device~~ is configured with at least one of an optical scanner and capacitance scanner.

9. (Currently Amended) The smartcard transaction system of claim 1, wherein said fingerprint sensor ~~device~~ is configured to detect and verify finger print minutia including at least one of ridge endings, bifurcation, lakes, enclosures, short ridges, dots, spurs, crossovers, pore size, pore location, loops, whorls, and arches.

10. (Currently Amended) The smartcard transaction system of claim 1, wherein said fingerprint sensor ~~device~~ is configured to include an additional sensor to detect and verify at least one of blood flow, correctly aligned ridges, pupil dilation, pressure, motion, and body heat.

11. (Cancelled)

12. (Currently Amended) The smartcard transaction system of claim ~~11~~ 1, wherein said verification device ~~configured to compare said fingerprint sample~~ is at least one of a third-party security vendor device and a local CPU.

13. (Cancelled)

14. (Cancelled)

15. (Currently Amended) The smartcard transaction system of claim ~~14~~ 1, wherein different registered fingerprint samples are associated with a different one of: personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information.

16. (Currently Amended) The smartcard transaction system of claim ~~14~~ 1, ~~wherein a fingerprint sample is primarily associated with first user information~~, wherein said first user account ~~information~~ comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account

information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information, and wherein ~~a fingerprint sample is secondarily associated with said second user information, wherein~~ said second user account ~~information~~ comprises at least one of personal information, credit card information, debit card information, savings account information, membership information, PayPal account information, Western Union Account information, electronic bill payment information, automatic bill payment information and loyalty point information~~, and wherein said second user information is different than said first user information~~.

17. (Original) The smartcard transaction system of claim 1, wherein said smartcard transaction system is configured to begin authentication upon verification of said proffered fingerprint sample.

18. (Original) The smartcard transaction system of claim 1, wherein said smartcard is configured to deactivate upon rejection of said proffered fingerprint sample.

19. (Currently Amended) The smartcard transaction system of claim 1, wherein said fingerprint sensor is configured to provide a notification upon detection of a sample, and wherein said notification is at least one of a notification to a security vendor, a notification to a store employee, and a notification to a primary account holder that said primary account is being accessed.

20. (Currently Amended) The smartcard transaction system of claim 1, wherein said verification device is further configured to facilitate at least one of access, activation of a device, a financial transaction, and a non-financial transaction.

21. (Currently Amended) The smartcard transaction system of claim 1, wherein said verification device ~~configured to verify~~ is configured to facilitate the use of ~~at least one~~ a secondary security procedure which includes sending a signal to said host to notify that a condition of use for said smartcard is being violated.

22. (Currently Amended) A method for facilitating biometric security in a smartcard transaction system comprising:

registering a fingerprint sample by primarily associating said fingerprint sample with a first user account and secondarily associating said fingerprint sample with a second user account to create a registered fingerprint sample, wherein said second user account is different than said first user account;

proffering a fingerprint to a fingerprint sensor communicating with said system to ~~initiate~~ form a proffered fingerprint sample;

selecting at least one of said first user account and said second user account to facilitate a smartcard payment transaction upon verification of ~~a~~ said proffered fingerprint sample against said registered fingerprint sample ~~for facilitating authorization of a transaction~~.

23. (Currently Amended) The method ~~for~~ of claim 22, ~~further comprising~~ wherein said step of registering ~~at least one fingerprint sample with~~ comprises contacting an authorized sample receiver.

24. (Currently Amended) The method of claim 23, wherein said step of registering further includes at least one of: ~~contacting said authorized sample receiver,~~ proffering ~~a~~ said fingerprint to said authorized sample receiver, processing said fingerprint to obtain ~~a~~ said fingerprint sample, ~~associating said fingerprint sample with user information,~~ verifying said fingerprint sample, and storing said fingerprint sample upon verification.

25. (Currently Amended) The method of claim 22, wherein said step of proffering includes proffering ~~a~~ said fingerprint to at least one of an optical scanner and a capacitance scanner.

26. (Currently Amended) The method of claim 22, wherein said step of proffering further includes proffering ~~a~~ said fingerprint to ~~a~~ said fingerprint sensor communicating with said system to initiate at least one of: storing, comparing, and verifying said fingerprint sample.

27. (Currently Amended) The method of claim 22, wherein said step of proffering ~~a fingerprint to a fingerprint sensor communicating with said system to initiate verification~~ further includes processing database information, wherein said database information is contained in at least one of a smartcard, smartcard reader, sensor, remote server, merchant server and smartcard system.

28. (Cancelled)

29. (Currently Amended) The method of claim ~~28~~ 22, wherein said step of ~~comparing~~ verifying includes comparing ~~a~~ said proffered fingerprint sample to ~~a stored~~ said registered fingerprint sample by using at least one of a third-party security vendor device and a local CPU.

30. (Currently Amended) The method of claim ~~28~~ 22, wherein said step of ~~comparing~~ verifying includes comparing fingerprint minutia.

31. (Currently Amended) The method of claim 30, wherein said step of comparing fingerprint minutia comprises storing, processing and comparing at least one of ridge endings, bifurcation, lakes, enclosures, short ridges, dots, spurs, crossovers, pore size, pore location, loops, whorls, and arches.

32. (Currently Amended) The method of claim 22, wherein said step of proffering ~~a fingerprint to a fingerprint sensor communicating with said system~~ further comprises using said fingerprint sensor to detect at least one of blood flow, correctly aligned ridges, pupil dilation, pressure, motion, and body heat.

33. (Currently Amended) The method of claim 22, wherein said step of proffering ~~a fingerprint to a fingerprint sensor communicating with said system to initiate verification~~ further includes at least one of detecting, processing and storing ~~at least one~~ a second proffered fingerprint sample.

34. (Currently Amended) The method of claim 22, wherein said step of proffering ~~a fingerprint to a fingerprint sensor communicating with said system to initiate verification~~ further includes the use ~~of at least one~~ a secondary security procedure which includes sending a signal to a host to notify that a condition of use for a smartcard is being violated.

35. (Currently Amended) A method for facilitating biometric security in a smartcard transaction system comprising:

receiving data from a smartcard via a reader which communicates with said system;

detecting a proffered fingerprint at a sensor ~~communicating~~ which communicates with said system to obtain a proffered fingerprint sample;

verifying ~~the~~ said proffered fingerprint sample by comparing said proffered fingerprint sample with a registered fingerprint sample, wherein said registered fingerprint sample is primarily associated with a first user account and secondarily associated with a second user account, and wherein said second user account is different than said first user account ~~to facilitate a transaction; and~~

using at least one of said first user account and said second user account to facilitate a smartcard payment transaction; and,

authorizing ~~a~~ said smartcard payment transaction to proceed upon verification of ~~the~~ said proffered fingerprint sample.

36. (Currently Amended) The method of claim 35, wherein said step of detecting further includes detecting ~~a~~ said proffered fingerprint at ~~a~~ said sensor ~~configured to communicate~~ which communicates with said system via at least one of ~~a~~ said smartcard, said reader, and a network.

37. (Currently Amended) The method of claim 35, wherein said step of detecting ~~a~~ said proffered fingerprint includes detecting ~~a~~ said proffered fingerprint by at least one of a capacitance scanner and an optical scanner.

38. (Currently Amended) The method of claim 35, wherein said step of detecting includes at least one of: detecting, storing, and processing ~~a~~ said proffered fingerprint sample.

39. (Currently Amended) The method of claim 35, wherein said step of detecting further includes receiving a finite number of proffered fingerprint samples ~~during a transaction~~.

40. (Currently Amended) The method of claim 35, wherein said step of detecting further includes ~~logging each proffered fingerprint sample.~~ storing log data information comprising at least one of a detected fingerprint sample, a processed fingerprint sample and said registered fingerprint sample, and wherein said fingerprint sensor is further configured to employ a security procedure when said proffered fingerprint sample differs from said log data information.

41. (Currently Amended) The method of claim 35, wherein said step of detecting further includes at least one of ~~detection~~ detecting, processing and storing ~~at least one~~ a second proffered fingerprint sample.

42. (Original) The method of claim 35, wherein said step of detecting further includes using said fingerprint sensor to detect at least one of blood flow, correctly aligned ridges, pupil dilation, pressure, motion, and body heat.

43. (Cancelled)

44. (Currently Amended) The method of claim ~~43~~ 35, wherein said step of comparing ~~a~~ said proffered fingerprint sample with ~~a stored~~ said registered fingerprint sample comprises storing, processing and comparing ~~at least one~~ fingerprint minutia.

45. (Currently Amended) The method of claim ~~43~~ 35, wherein said step of comparing ~~a~~ said proffered fingerprint sample with ~~a stored~~ said registered fingerprint sample includes comparing ~~a~~ said proffered fingerprint sample with a biometric sample of at least one of a criminal, a terrorist, and a cardmember.

46. (Currently Amended) The method of claim 35, wherein said step of verifying includes verifying ~~a~~ said proffered fingerprint sample using information contained on at least one of a local database, a remote database, and a third-party controlled database.

47. (Currently Amended) The method of claim 35, wherein said step of verifying includes verifying ~~a~~ said proffered fingerprint sample using at least one of a local CPU and a third-party security vendor.

48. (New) The smartcard transaction system of claim 1, wherein said proffered fingerprint sample is further configured as at least one of a variable in an encryption calculation to secure data, and as both a private key and a public key for encryption purposes.

49. (New) The method of claim 22, further comprising using said proffered fingerprint sample as at least one of a variable in an encryption calculation for securing data, and as both a private key and a public key for encryption purposes.